Integrating OT Cyber Security Throughout the Project Lifecycle

Paper No. PCIC Europe EUR24_27

Anusha Challa
Wintershall Dea
Friedrich-Ebert-Straße 160
34119 Kassel
Germany

Norman Blume
Wintershall Dea
Friedrich-Ebert-Straße 160
34119 Kassel
Germany

Abstract - In today's interconnected landscape, we emphasize the critical imperative of proactively integrating Operational Technology (OT) security from a project's inception and seamlessly weaving it through every project phase. This paper delves into comprehensive strategies, including risk assessments, vulnerability assessments, and adherence to industry standards, to fortify critical infrastructure. By systematically addressing these key elements, organizations enhance operational resilience, minimize vulnerabilities, ensure compliance, and foster project success, safeguarding operations.

This paper describes our experience in an own operated subsea gas project with the Tie-In into an existing Topside Platform of another operator. It also describes how this experience can be incorporated into a new expansion of this subsea gas production and how new approaches will increase the safety of the overall system. The fact that these changes will also affect the existing facilities and that concepts will have to be developed for an overall offshore modification is always taken into account.

Index Terms — OT Security, Project Lifecycle, Perdue model, Risk Assessment.

I. Background

Operational Technology (OT) encompasses the hardware and software used to monitor and control physical devices, processes, and infrastructure. In critical infrastructure projects, such as subsea gas developments, OT systems play a vital role in ensuring operational efficiency and safety. However, the increasing connectivity of OT systems exposes them to cybersecurity risks, including unauthorized access, data breaches, and operational disruptions. Addressing these risks requires proactive measures to integrate robust security controls into the project's design, implementation, and maintenance phases.

II. Objectives

The objective of this paper is to:

- *Explore comprehensive strategies for integrating OT security from project inception.*
- *Discuss the importance of risk assessments, vulnerability assessments, and adherence to industry standards in fortifying critical infrastructure projects.*
- *Highlight the benefits of systematically addressing key elements to enhance operational resilience, minimize vulnerabilities, ensure compliance, and foster project success.*

III. Integrating OT Cybersecurity in Different Phases of Project

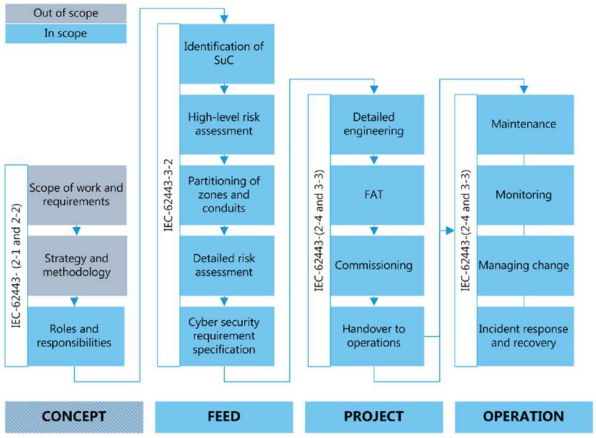

Fig.1: IEC 62443 in FEED production and operation

Concept Phase:

- *Establishing high-level security requirements aligned with project objectives and industry standards.*
- *Incorporating OT cybersecurity considerations into the project's conceptual design and feasibility studies.*

FEED (Front End Engineering Design) Phase:

- *Preliminary risk assessments to identify potential security threats and vulnerabilities.*

The objectives of this assessment are to:

- Identify risks associated with IACS system that directly or indirectly perform functions protecting against major accident, risk or loss of essential production service.
- Take a precautionary approach without unnecessarily precluding beneficial technologies allow countermeasures to be modified as technologies develop alongside intelligence on threats and vulnerabilities.
- Define defence in depth approach for IACS system hardware and software.

Parties involved in Feed phase Risk Assessment

- *Project Team*
- *OT Security Experts*
- *Operations and Maintenance Personnel*
- *EPC Contractor*
- *Host Operator*

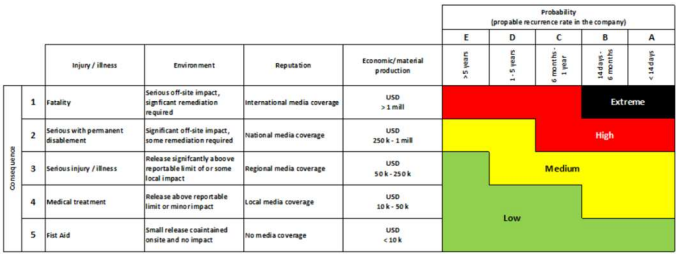

Fig.2: Qualitative Risk Matrix

Risk	Vulnerabilities and Consequences
Denial of Control	Temporarily prevents operators and engineers from interfacing with process controls. An affected process may still be operating during the period of control loss, but not necessarily in a desired state.
Manipulation of Control	Unauthorized changes made to programmed instructions in PLCs, RTUs, DCS, or SCADA controllers, alarm thresholds changed, or unauthorized commands issued to control equipment, which could potentially result in damage to equipment (if tolerances are exceeded), premature shutdown of processes (such as prematurely shutting down transmission lines), causing an environmental incident, or even disabling control equipment.
Spoofed Reporting Message	False information sent to an OT system operator either for evasion or to impair process control. The adversary could make the defenders and operators think that other errors are occurring in order to distract them from the actual source of the problem (i.e., alarm floods).
Theft of Operational Information	Adversaries may steal operational information for personal gain or to inform future operations.
Loss of Safety	Adversaries may target and disable safety system functions as a prerequisite to subsequent attack execution or to allow for future unsafe conditionals to go unchecked.
Loss of Availability	Adversaries may leverage malware to delete or encrypt critical data on HMIs, workstations, or databases.

Table 1: High Level Risks

- *Developing high level security architectures and designs tailored to project specifications and operational needs.*

Purdue Model:

The Purdue Model, also known as the Purdue Enterprise Reference Architecture, is a hierarchical model that organizes ICS infrastructure into different levels based on functionality, data flow, and security considerations. It provides a structured approach to understanding and securing ICS environments, offering clear boundaries and guidelines for implementing security controls.

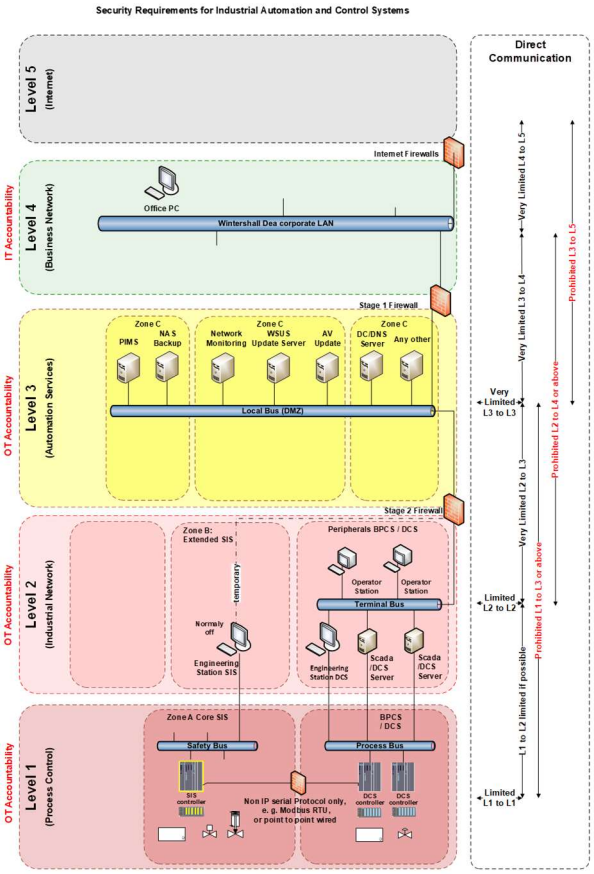

Fig.3: Purdue Model: Network layered Architecture Design

Project / Execution Phase:

- *Conducting comprehensive risk assessments and vulnerability analyses to identify specific security requirements.*

ESTABLISHING TARGET SECURITY LEVELS

Security Levels (SL) provide a qualitative approach to addressing security for a zone. As a qualitative method, security level definition has applicability for comparing and managing the security of zones within an organization.

It should established that the security level of the supplied equipment is SL2 or below (As part of case study)

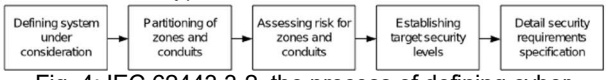

Fig. 4: IEC 62443 3-2, the process of defining cyber security requirements.

- *Implementing secure network architectures and access controls to protect critical assets and infrastructure.*
- *Ensuring compliance with industry standards and regulatory requirements governing OT cybersecurity.*

Operation Phase:

- *Providing comprehensive training and awareness programs for project personnel to mitigate human-related risks.*

IV. CASE STUDY

The scope of the project included the installation of subsea production facilities, and control systems, as well as the integration of OT security measures to protect critical assets and infrastructure.

Throughout the project lifecycle, OT security was integrated into every phase, from conceptual design and engineering to construction, commissioning, and ongoing operations. Key strategies employed included:

- Implementing secure network architecture to segregate OT systems from external threats.
- Conducting regular security audits and assessments to identify and remediate vulnerabilities.
- Providing comprehensive training and awareness programs for project personnel to mitigate human-related risks.

Compliance to Regulations:

In addition to internal security standards and best practices, the project prioritized compliance with relevant regulations and industry standards governing OT security in critical infrastructure projects. This included adherence to regulations such as the International Society of Automation (ISA) 62443 series, NIST Special Publication 800-82, and industry-specific guidelines and directives. By aligning with regulatory requirements, the project demonstrated its commitment to maintaining high standards of security and resilience, thereby mitigating legal and regulatory risks associated with non-compliance.

Introduction of Virtualization Technology:

To enhance security and improve control over third-party access, the project introduced virtualization technology. Separate virtual machines (VMs) were created for each third-party vendor, providing dedicated environments for their applications and services. This approach enhanced security by isolating vendor-specific software and data, minimizing the risk of unauthorized access or data breaches. Additionally, virtualization facilitated centralized management and monitoring of vendor environments, enabling real-time visibility into their activities and enhancing overall security posture.

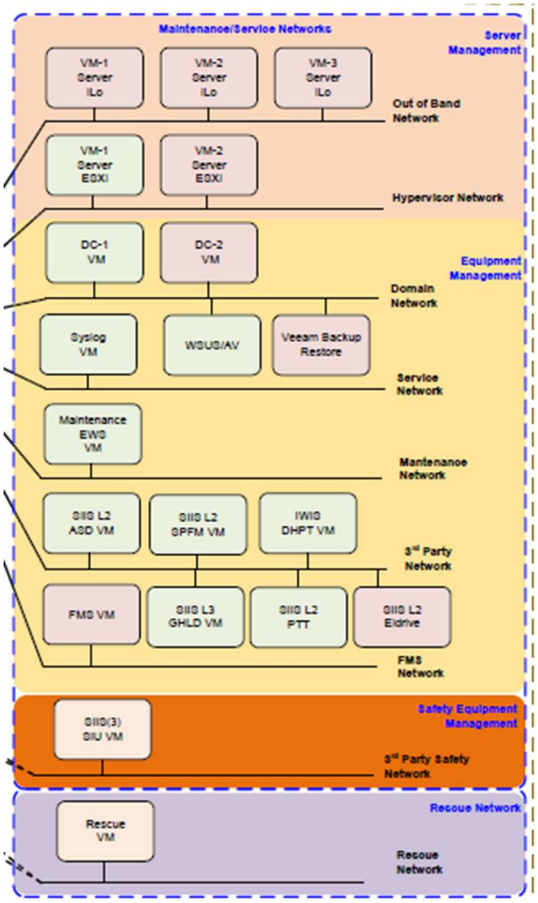

Fig. 5: Separation of Virtual Machines into different Zones

Standard Network Architecture:

The project adopted a standard network architecture tailored to the specific requirements of OT systems, facilitating secure communication and data exchange between devices and control centres. The architecture incorporated principles of defence-in-depth, segmentation, and isolation to mitigate the impact of cyber attacks and limit the propagation of threats within the network. By implementing standardized network architectures, the project ensured consistency, interoperability, and scalability while maintaining a strong security posture across the infrastructure.

Level 5: Enterprise Network

- Corporate-level services supporting individual business units and users. These systems are usually located in corporate data centers.

Level 4: Business Networks

- IT networks for business users at local sites. Connectivity to Enterprise wide area network (WAN) and possibly local Internet access. Direct Internet access should not extend below this level.

Level 3.5: Demilitarized Zone (DMZ)

- The DMZ acts as a buffer between IT and OT networks, containing firewalls and security systems to control data flow.
- It ensures controlled communication between Levels 4/5 and Levels 0-3, reducing cyber risk.

Level 3: Site-Wide Supervisory

- This Level manages production workflows with systems such as Manufacturing Execution Systems (MES).
- It helps optimize production and collects real-time data for analysis.
- Components: Metering Systems, Historians, Alarm Servers

Level 2: Supervisory Control

- This level focuses on monitoring and supervisory control of the production process.
- Components: Human-Machine Interfaces (HMIs), Supervisory Control and Data Acquisition (SCADA) systems, and other control systems that oversee the operation of Level 1 devices.

Level 1: Basic Control

- This level involves the control of the physical processes.
- Components: Programmable Logic Controllers (PLCs), Remote Terminal Units (RTUs), and Distributed Control Systems (DCSs).

Level 0: Physical Process

- This level encompasses physical processes and devices such as sensors, actuators, and other physical equipment that perform the production tasks.
- Components: Sensors (e.g., temperature, pressure, flow), actuators (e.g., valves, motors).

Zones and Conduits

The intention of grouping assets into zones and conduits is to identify those assets which share common characteristics and security requirements, these are known as its attributes and typically take the form of the following:

- *security policies*
- *asset inventory*
- *access requirements and controls*
- *threats and vulnerabilities*
- *consequences of a security breach*
- *authorized technology*

Allocating equipment into zones with common attributes permits the identification of common security measures required to mitigate the risk.

Zones

A zone is defined as a grouping of logical or physical assets that share common security requirements, based on factors such as criticality or consequence.

Conduits

Conduits control access to zones and can be a single service (for example a single Ethernet network) or it can be made up of multiple data carriers (for example multiple network cables).

Points to consider for Tie-in projects:

Adhering to Host Operator's Requirements:

- Ensure compliance with the security standards, regulations, and contractual obligations set forth by the host operator.

Leveraging Existing Topside Infrastructure:

- Evaluate the feasibility of utilizing the existing topside Windows and antivirus update servers, NTP server(Network Time Protocol) for seamless integration.
- Utilizing existing SOC (Security Operations Centre) and Incident response process
- Ensure compatibility with host operator's infrastructure while maintaining security and regulatory compliance.

Implementing Remote Access Solutions:

- Incorporate a robust remote access solution to facilitate maintenance, monitoring, and troubleshooting activities.
- Align remote access mechanisms with host operator's security protocols and standards to ensure secure connectivity.

Optimizing Backup Procedures:

- Assess the feasibility of conducting backups locally and subsequently transferring them to a centralized backup server.
- Establish secure procedures for backup storage and transmission

Alignment with all the involved parties:

- Project team shall align with Operators and Host operators and involve them in the necessary meetings in each phase of the project.

V. CONCLUSIONS

In conclusion, the integration of OT security is a vital component of modern critical infrastructure projects. By incorporating robust security measures from project inception and throughout the project lifecycle, organizations can mitigate risks, ensure compliance, and safeguard their operations against cyber threats. The case study presented in this paper demonstrates the efficacy of such an approach in a real-world scenario and highlights the importance of proactive risk management and security integration in critical infrastructure projects.

VI. ACKNOWLEDGEMENTS

The author would like to thank Diedrich Thaden and the PCIC Technical committee for their review.

VII. REFERENCES

[1] IEC 62443: Recommended Practice
Cyber security in the oil and gas industry based on IEC 62443
[2] DNV-RP-G108: Recommended Practice
Cyber security in the oil and gas industry based on IEC 62443
[3] NIST 800-82 R3: NIST
Guide to Operational Technology (OT) Security

VIII. VITA

Anusha Challa graduated from the Visvesvaraya Technological University (VTU) in 2011 with a degree in Instrumentation Technology. She possesses over a decade of experience in the engineering domain. With roles encompassing DCS engineering and specialization in OT security. Additionally, she owns 4 patents on OT Network and security.
anusha.challa@wintershalldea.com

Norman Blume graduated from the University of Applied Sciences Flensburg in 2006 with a Diploma in Electrical Engineering. He has many years of experience as a project engineer and as an Electrical Department Manager of Onshore & Offshore Oil production facilities and electrical engineering teams.
norman.blume@wintershalldea.com